CHAPTER 2

SYSTEMS ENGINEERING CONSIDERATIONS

2-1. General systems considerations

Requirements are presented in this manual for the design of optimally reliable mechanical and electrical systems at command, control, communications, computer, intelligence, surveillance, and reconnaissance (C4ISR) facilities. These systems shall be capable of supplying services continually to the C4ISR installation site during any natural or man-made disruption in commercial services. Off-site power facilities are assumed to be adequate to supply peak power demands, but are not assumed to be uninterruptible. Potential threats include physical attacks; biological, chemical, and radiological warfare; and close-in and high-altitude nuclear blasts.

2-2. Program elements

The essential elements of a systems engineering program are described below.

a. Reliability, availability, and maintainability (RAM). During design, the design agency shall implement RAM requirements to maximize the availability of the C4ISR systems.

b. Human factors engineering (HFE). HFE activities will ensure that reliability, availability, and safety of the C4ISR systems are not degraded through human activities during operation or maintenance. The design agency shall accomplish the HFE program requirements through the use of established standard HFE design criteria and practices based on MIL-STD-1472, Human Engineering Design Criteria for Military Systems, Equipment, and Facilities.

c. System safety. The C4ISR power system safety program shall ensure that the design incorporates, within program restraints, the highest attainable level of inherent safety. It shall eliminate or reduce the probability of events that can cause injury or death to personnel, or damage to or loss of equipment or property. For example, pipes, lines, and tanks shall be placed away from high-traffic areas. Safety documentation shall be provided for safety items that require designation or may cause action during subsequent program phases. The design agency system safety program shall be based on a philosophy that the most effective actions to control potential hazards are those taken early in the design process.

(1) When hazards cannot be controlled by design measures, including safety and warning devices, special operating procedures shall be developed and documented. The safety program shall provide support to the systems engineering (SE) program and shall ensure that the applicable requirements of MIL-STD-882, System Safety Program Requirements, are met.

(2) The systems safety program shall define and address the safety analyses that shall be performed during development of design. During the early design phase, an analysis that identifies conditions that may cause injury or death to personnel and damage or loss to equipment and property shall be performed. Prior to the final safety design review, the design agency shall perform a second systems safety analysis to determine adherence of the design to all required safety standards and criteria, and to ensure avoidance or reduction of identified hazards. Operating and maintenance procedures shall also be reviewed for compliance with all required safety standards and criteria.

(3) The systems safety program shall include follow-up/corrective procedures to ensure that safety hazards identified by the systems safety analyses are eliminated or reduced to acceptable levels of risk, and that actions taken are fully documented.

(4) The design agency shall prepare specific safety program documentation. This documentation shall include, but not be limited to, safety analysis reports and the final systems safety report.

d. Consolidated system testing. The design agency shall develop a consolidated systems test program that covers all phases of testing, develops confidence in the system, and provides means for interim and final acceptance of equipment and systems. The design agency shall minimize cost through elimination of testing duplication and by maximizing the collection of data for each test. Final acceptance of the system shall follow 100 percent successful completion of these tests.

e. Standardization. The design agency shall develop and implement a standardization program to minimize equipment and component stockage. Redundant systems shall be of the same design.

f. Configuration management (CM). The CM program shall maintain effective control over design from criteria development through design, construction, and installation of the equipment. A government configuration control procedure shall be developed by the design agency for use in the C4ISR configuration control program.

g. Operations and maintenance (O&M) planning. The design agency shall identify and recommend essential items of the program during the design phase. Basic elements of the program are as follows.

(1) Data requirements shall be identified for preparation of O&M manuals. Systems functional descriptions shall be developed. Requirements shall be developed for data collection, including repair parts list, calibration requirements, special tools and test equipment, repair parts stockage level, and shelf life data. Repair parts list, repair parts stockage level, test equipment, and test frequency shall be provided the using government agency.

(2) Systems and equipment of high complexity or peculiarity shall be identified, and special training for personnel who operate and maintain such systems and equipment shall be identified.

(3) The design agency shall identify those items critical to accuracy and repeatability, and shall recommend calibration requirements. Unique calibration requirements and procedures shall be provided whenever necessary.

(4) Systems test and checkout requirements to be performed following major maintenance activities shall be developed during design to ensure safe and normal operation of the system.

2-3 System Design Considerations

a. Offsite electrical power. Two separate commercial power sources are preferred in conjunction with redundant feeders between the commercial power substations and the C4ISR site power plant. When two separate transmission lines are not available, a single commercial power source could be used to supply redundant distribution feeders to the power plant. The redundancy should be provided through two or more full capacity feeders which will be supplied from normally isolated switchgear busses in the commercial power substation. If the two transmission lines are used, they should be supplied by the same utility company; if owned by different companies, they should be supplied from the same transmission grid system to ensure synchronism of the two transmission lines.

b. Onsite electrical power. Operational onsite units should be capable of supplying the peak site demands while operating independent of any commercial power source when loaded between 60 to 80 percent of their rated load capacities. Loading of active generating units should not exceed these percentages since the emergency shutdown of one unit could cause overloading and consequent shutdown of the other units. On the other hand, onsite generators should not be loaded below 50 percent of the kilowatt rating to prevent accumulation of acid and carbon (wet stacking). Onsite power system shall also be capable of making the transition from offsite to onsite power mode of operation in not more than one minute, including starting and synchronizing a sufficient number of generators to serve the required loads. Onsite power units shall be capable of being started using only onsite equipment and facilities.